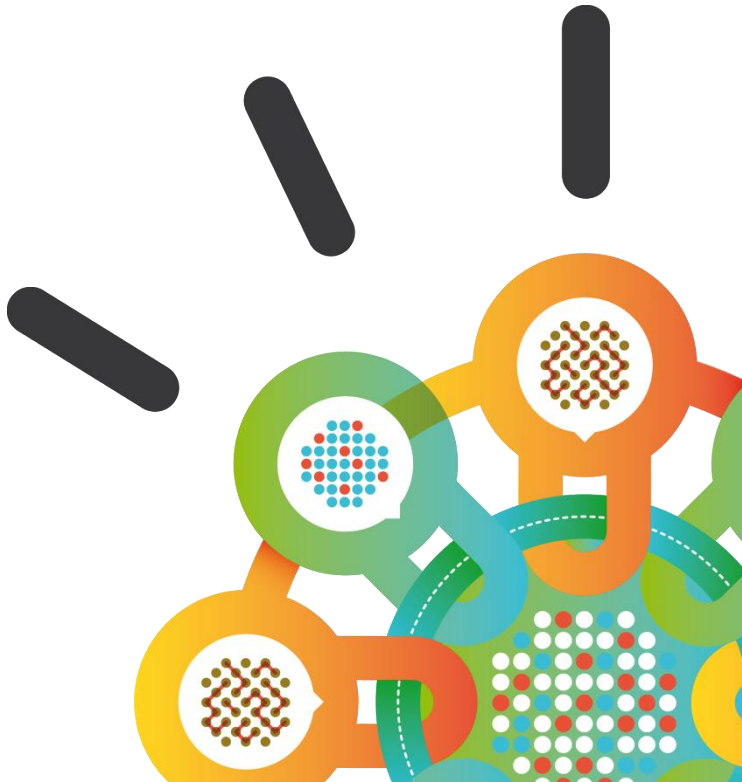
Security Intelligence.
Think Integrated.

Protect Your Organization from Your Biggest Threat – Insiders

Identity & Access Management

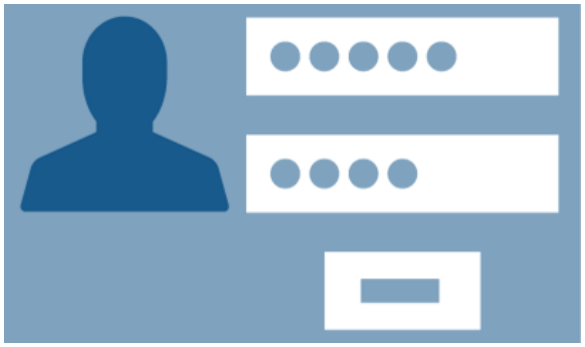
Brandon Whichard
Product Marketing
IBM Security

May 28, 2015



How are credentials compromised?

Usernames and Passwords will be stolen



Phishing

Identity and Access Management

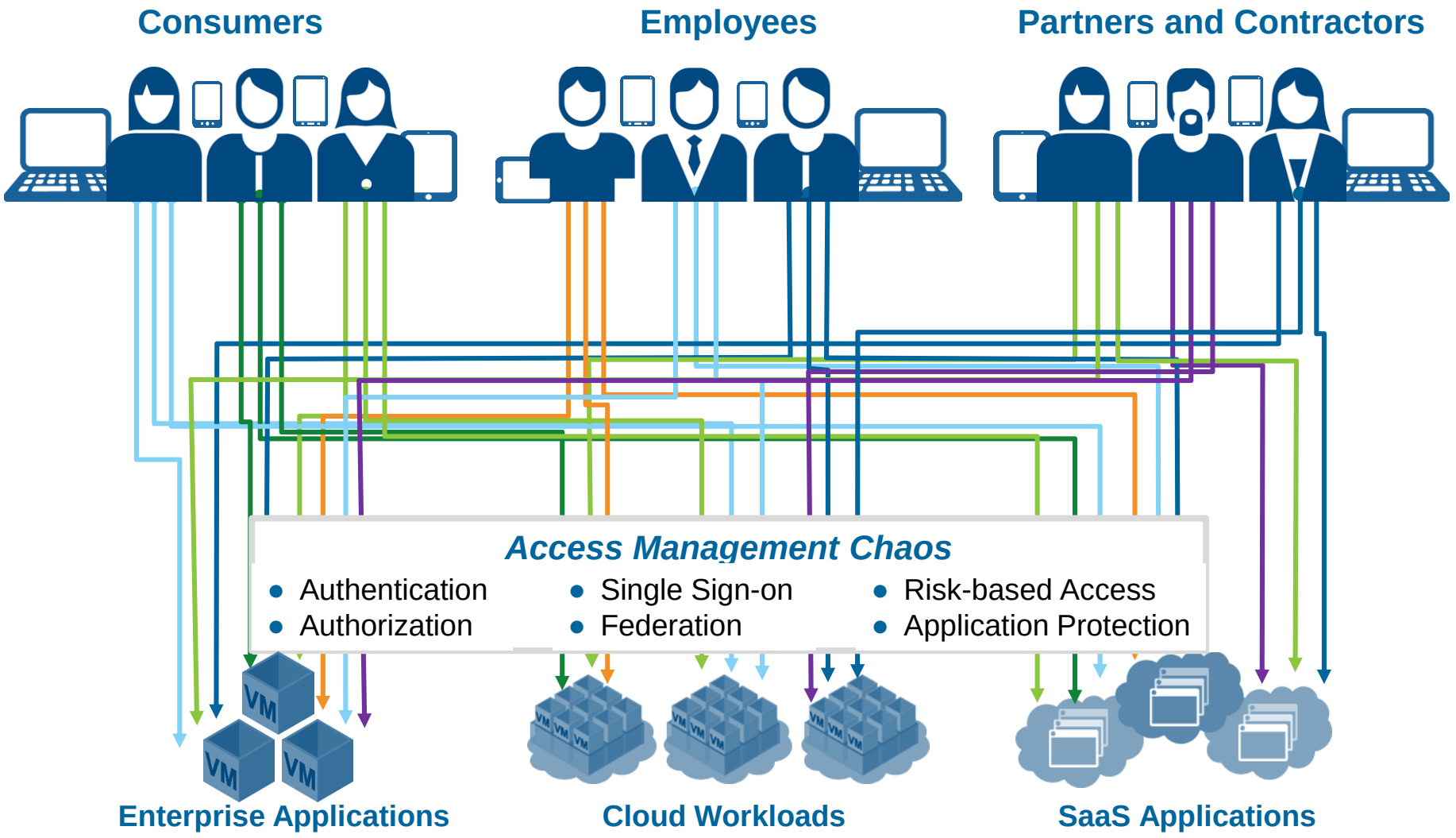
Govern and administer users and their access

<Identity Management>
Control unauthorized access and prevent "entitlement creep"

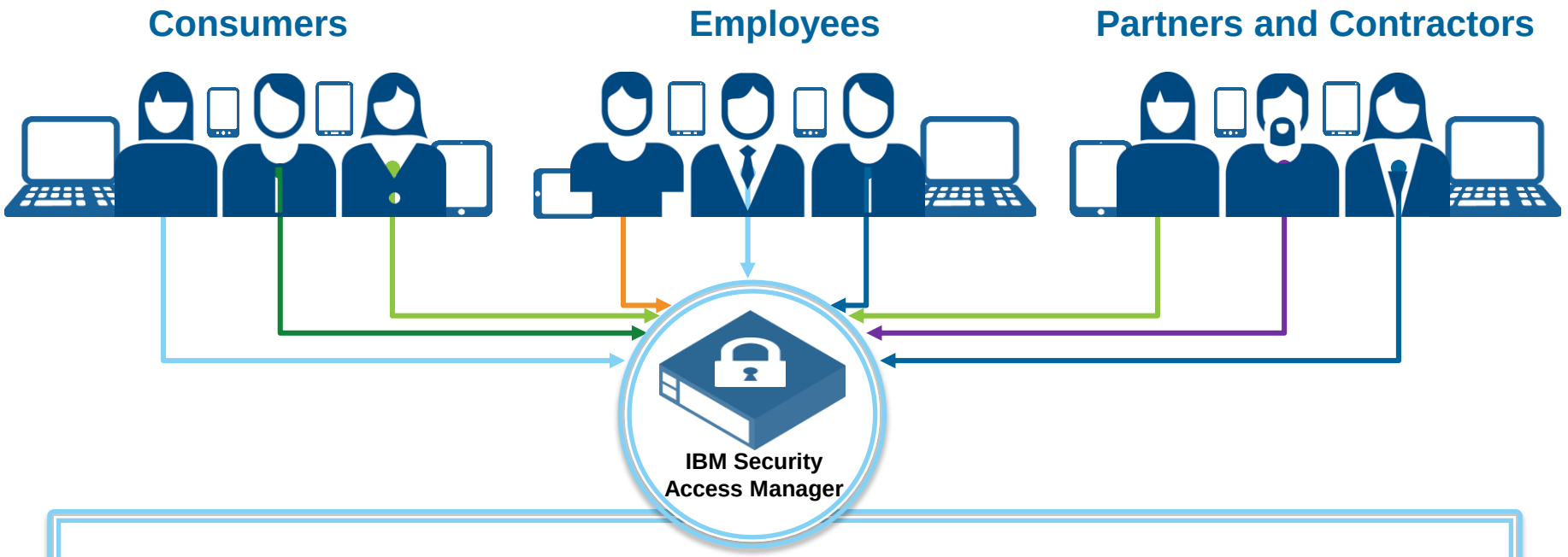
<Access Management>
Validate "who is who" across the enterprise and the cloud

1. ***Is this really a valid user?***
2. ***What does the user want to do?***
3. ***What access does that user need to do their job?***

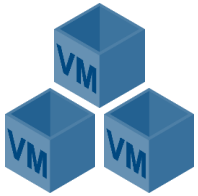
Access Management environments are becoming highly fragmented and complex, making enterprises less secure



Take back control of Access Management



- Authentication
- Authorization
- Single Sign-on
- Federation
- Risk-based Access
- Application Protection



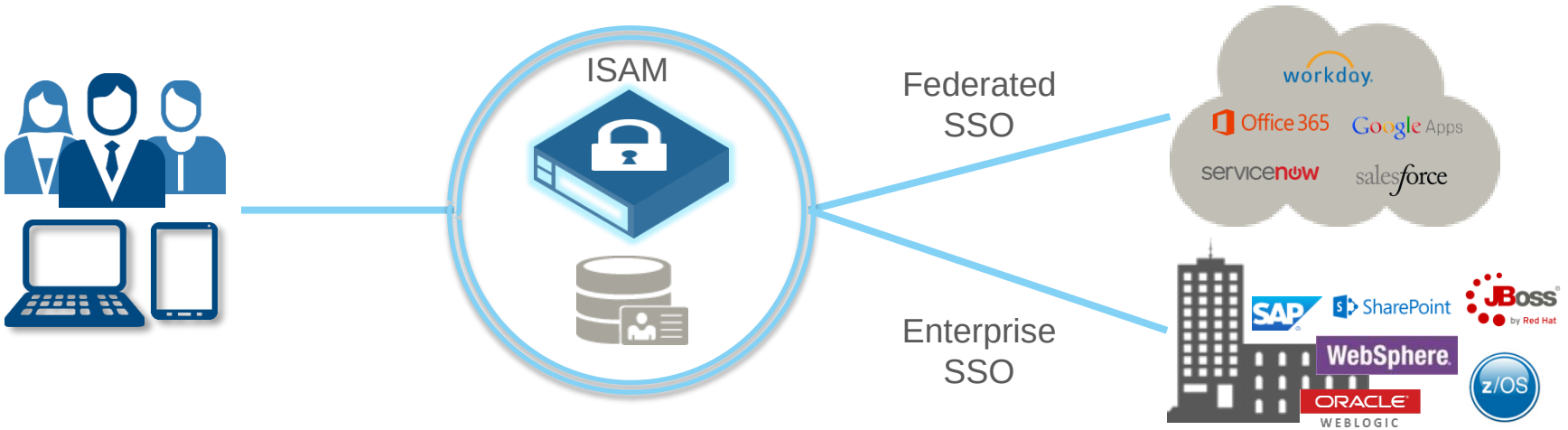
Enterprise Applications

Cloud Workloads

SaaS Applications

1. Manage access in the world of hybrid cloud

Enable SSO and identity federation to apps running inside & outside of the enterprise



- Quickly establish single sign-on connections to popular SaaS applications
- More easily create custom application connectors with Do-It-Yourself federations based on SAML 2.0 standard
- Deliver single sign-on to enterprise applications and support user identity propagation in hybrid cloud application interactions

3. Risk-aware access security for mobile apps and APIs

Transparently register mobile devices and enforce user-centric authentication policies

- Dynamically assess risk associated with mobile app access using contextual information about the device, user, environment, resource, and past user behavior
- Adaptive authentication improves mobile security posture while providing the least obtrusive end user experience
- Audit or block fraudulent and high-risk transactions from infected devices without modifying backend applications

CLIENT EXAMPLES

Risk-Based Access

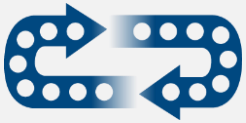
Large bank protects user access to apps from mobile and web channels for

Over 750K

users

Uses risk-based access, device registration and strong authentication

Performance & Scale



Large state agency needed to authenticate

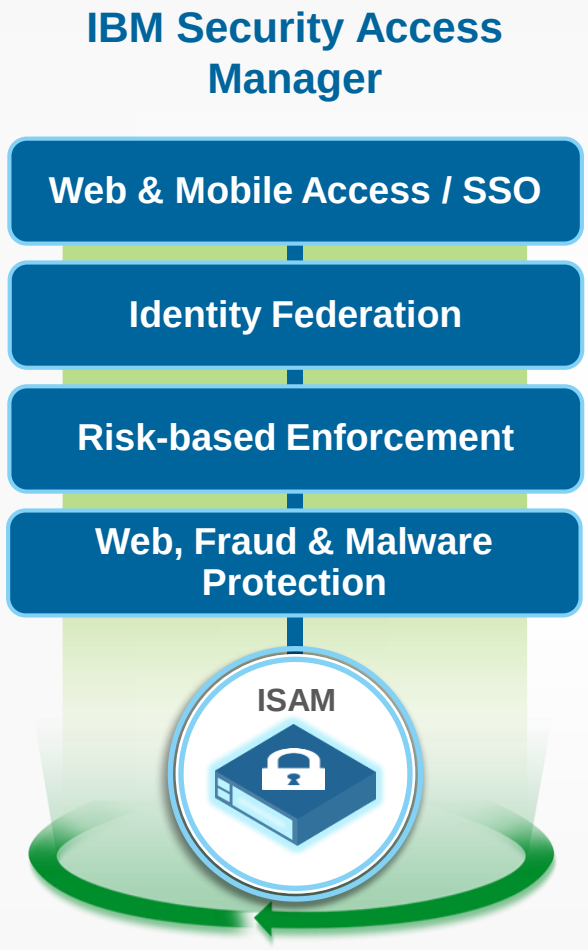
Over 10M

users

Major concern was to scale as user base grows and registrations increase

IBM Security Access Manager

Take back control of access management



- **Reduce TCO and time to value** with an modular “all-in-one” access appliance in virtual and hardware form factors
- **Deliver a multi-channel access gateway** to help secure employee and consumer access to mobile, web, APIs, and SaaS applications
- **Enforce identity- and risk-aware application access** for web and mobile devices
- **Secure identity assurance** with built-in mobile authentication service, one-time-password use
- **Deploy identity federation rapidly** using pre-integrated connectors to popular SaaS applications
- **Centrally manage policies** to protect enterprise from fraud and malware via Trusteer without modifying apps and risks associated with OWASP top 10 vulnerabilities
- **Deliver built-in integrations** with, MobileFirst Platform, MobileFirst Protect, Microsoft Office 365, SAP, Websphere and more

Identity and Access Management

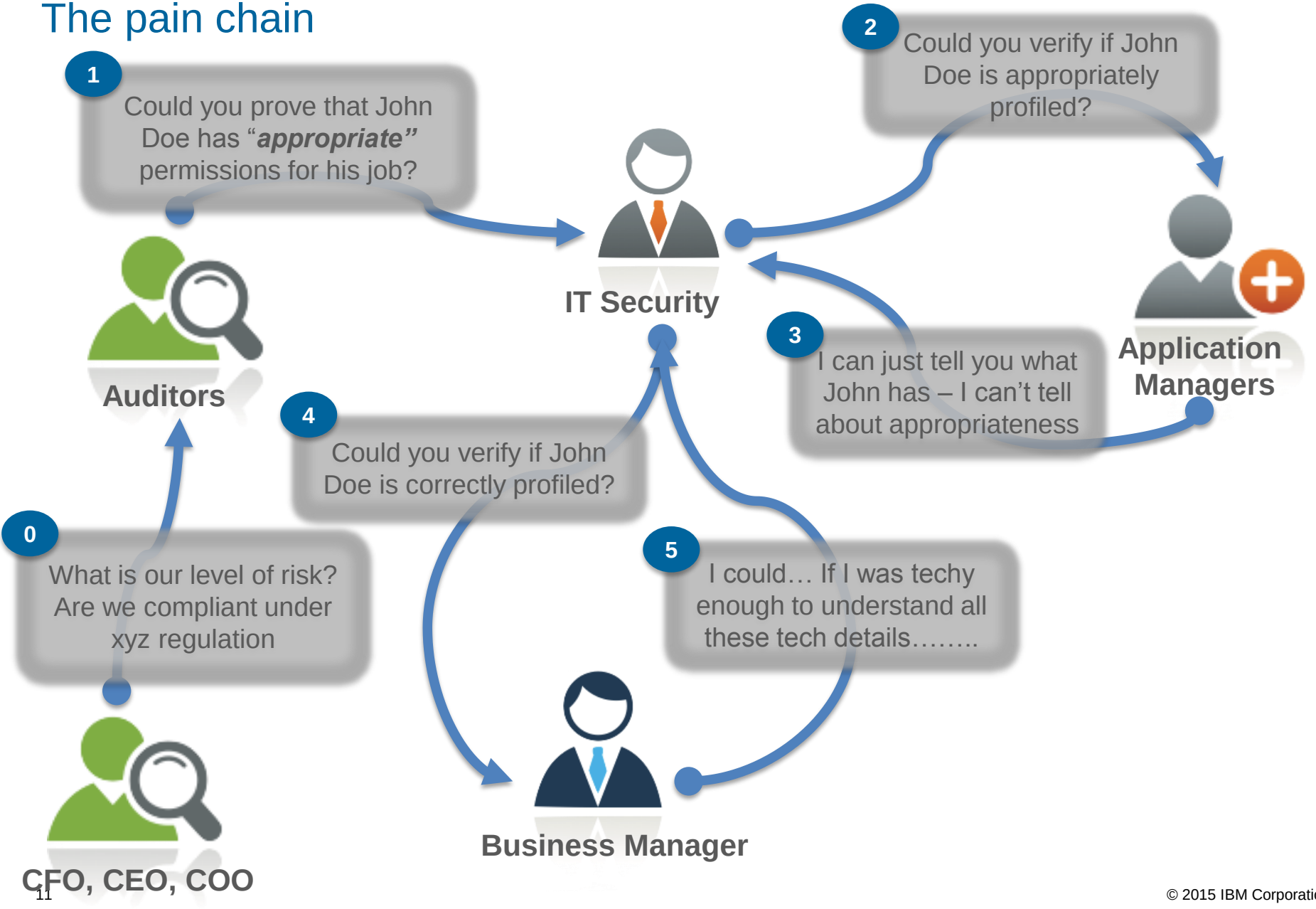
Govern and administer users and their access

<Identity Management>
Control unauthorized access and prevent "entitlement creep"

<Access Management>
Validate "who is who" across the enterprise and the cloud

1. ***Is this really a valid user?***
2. ***What does the user want to do?***
3. ***What access does that user need to do their job?***

The pain chain



The dependencies of traditional identity management

Business activities vs. Entitlements

Business Manager

Understands what **business activities** employees need

Requests employee IT entitlements from IT Security Manager

Which entitlements grant access to which business activities?

IT Security Manager

Provides information regarding who has which **entitlements**

Who SHOULD have which entitlements?

CRM	ERP
Mainframe	HR
Application Entitlements	

Auditor

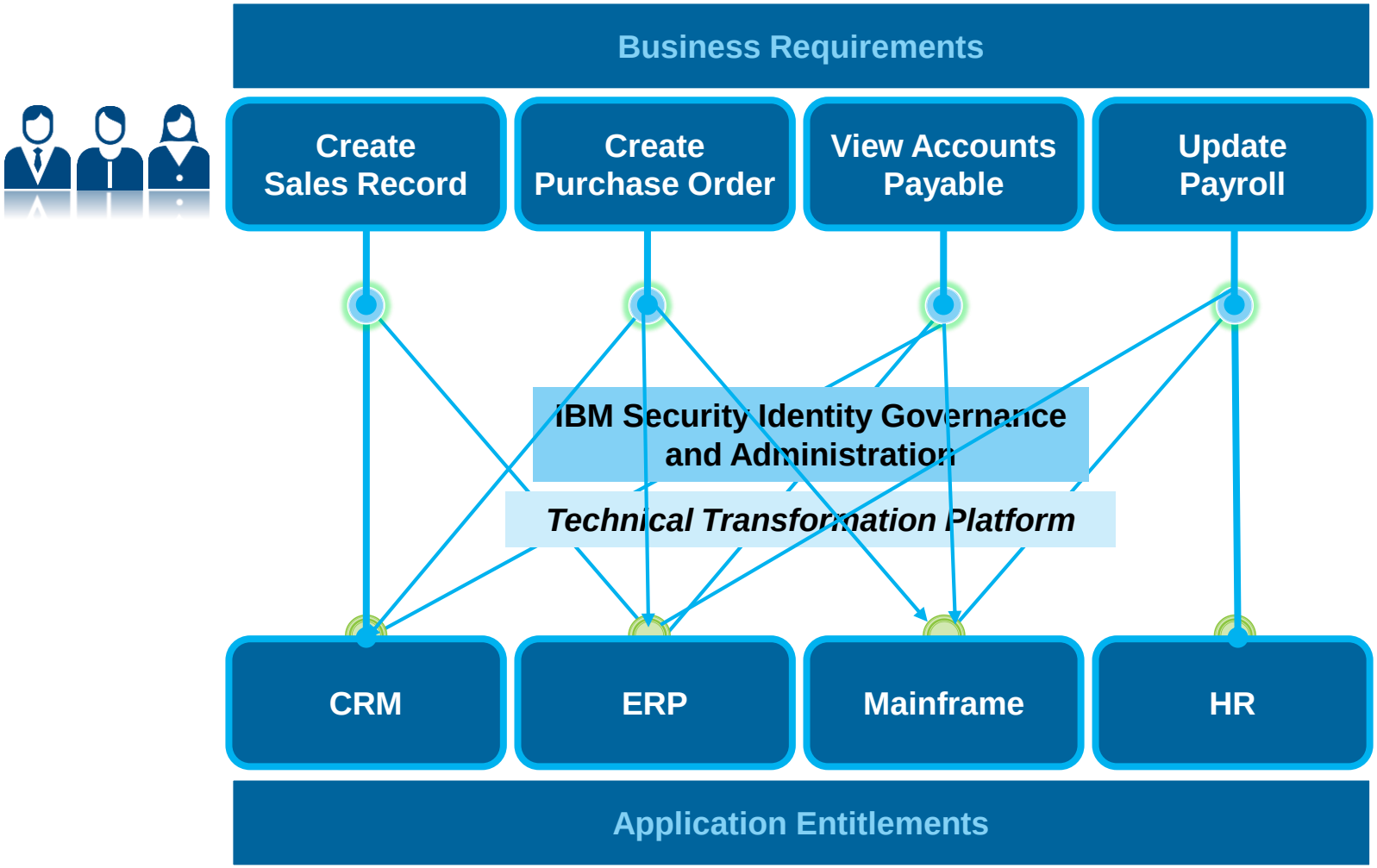
Identifies what **business activities** cause SoD violations *(toxic combinations)*

Receives list of entitlements based on IT Security Manager's request

Which entitlements cause toxic combinations?

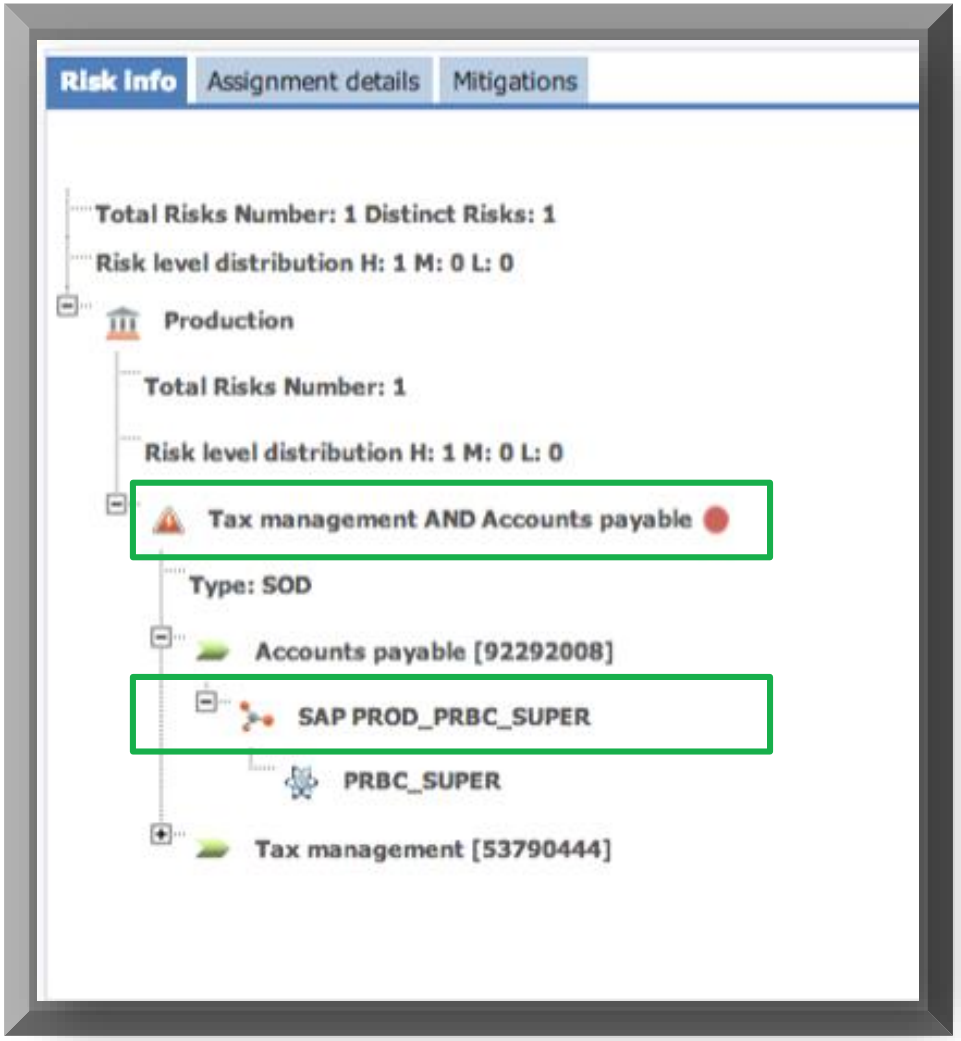
The IBM Security Identity Management Approach

Automatically map entitlements to Business activities



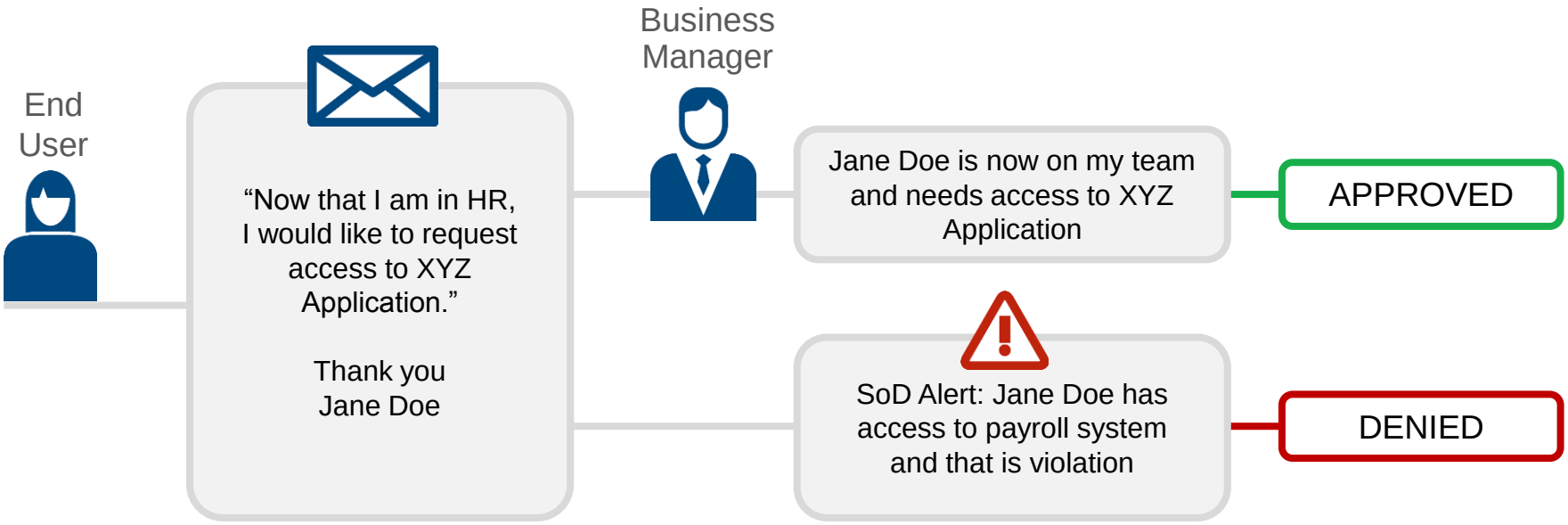
Simplified separation of duty modeling

- Auditors build rules from the top down starting with “Business Activity”
- IT maps the actual entitlements related to business activity
- Auditors may create, update and delete SoD rules without IT intervention
- IT can map new entitlements to business activities *one time*



1. Access request management

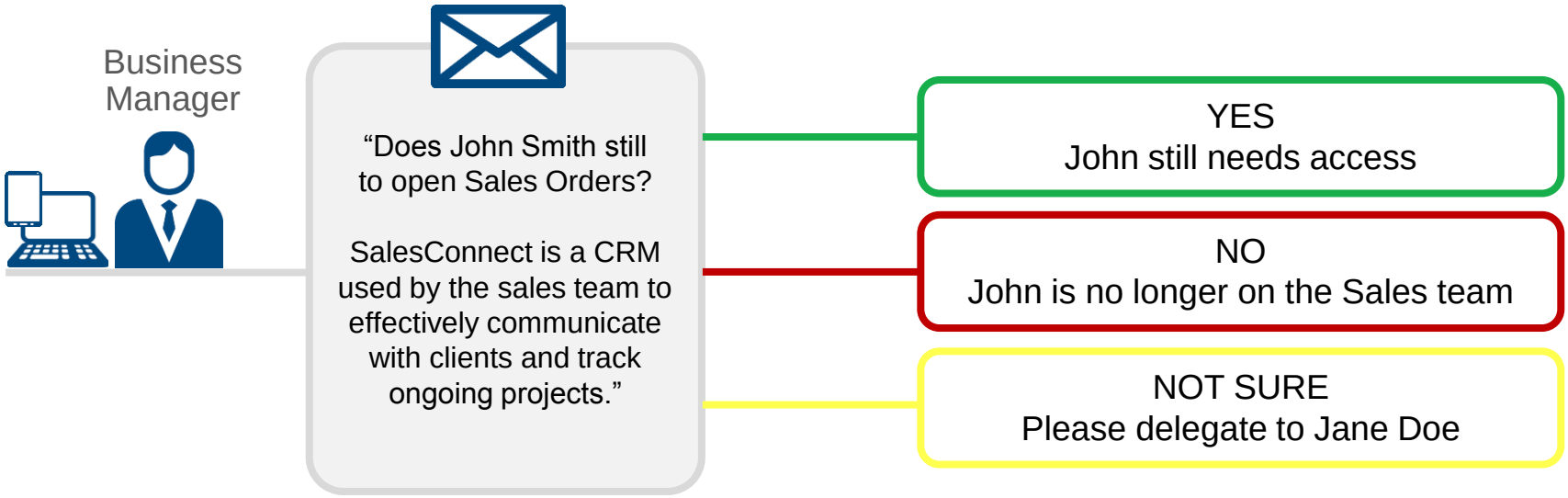
Allow users to quickly and effectively request their own access



- Self-service, shopping cart model
- Features multiple paradigms: business role, IT / application role, "Like Mike"
- Automatically alerts users when there is a separations of duties (SoD) conflict
- Saves time and money, while keeping the organization secure and compliant

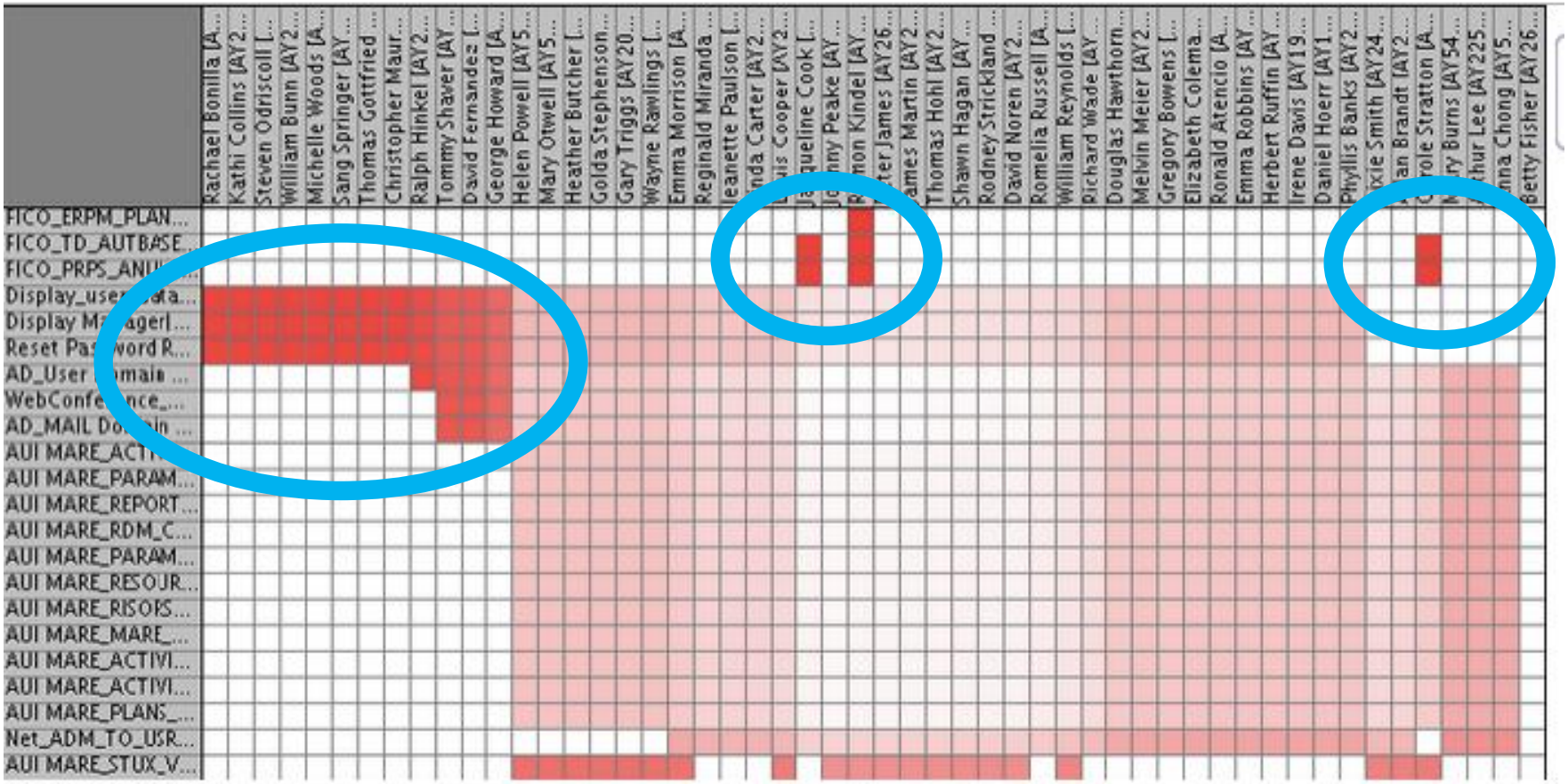
2. Access certification

Use business language to take quick and effective action regarding user access



- Focused, risk-driven campaigns
- Business language is used so the business manager can understand exactly what entitlements he is certifying and take the appropriate action
- Support business manager's decision making to certify user access

Identifying Outliers and Assessing Risk



Identity Governance and Administration Results

CLIENT EXAMPLES

Audit Access

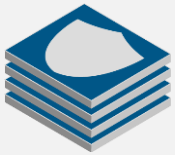
Large European designer found almost

80%

of users had unnecessary access

after leveraging the "last usage" information in their automated controls set

Governance



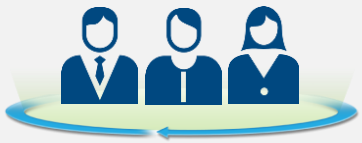
Large European insurance and financial services firm governs access to

75,000

employees, agents, privileged users

by identifying access risks, separation of duty and certify access for SAP, AD, mainframe, and custom-built apps

SoD Simplification



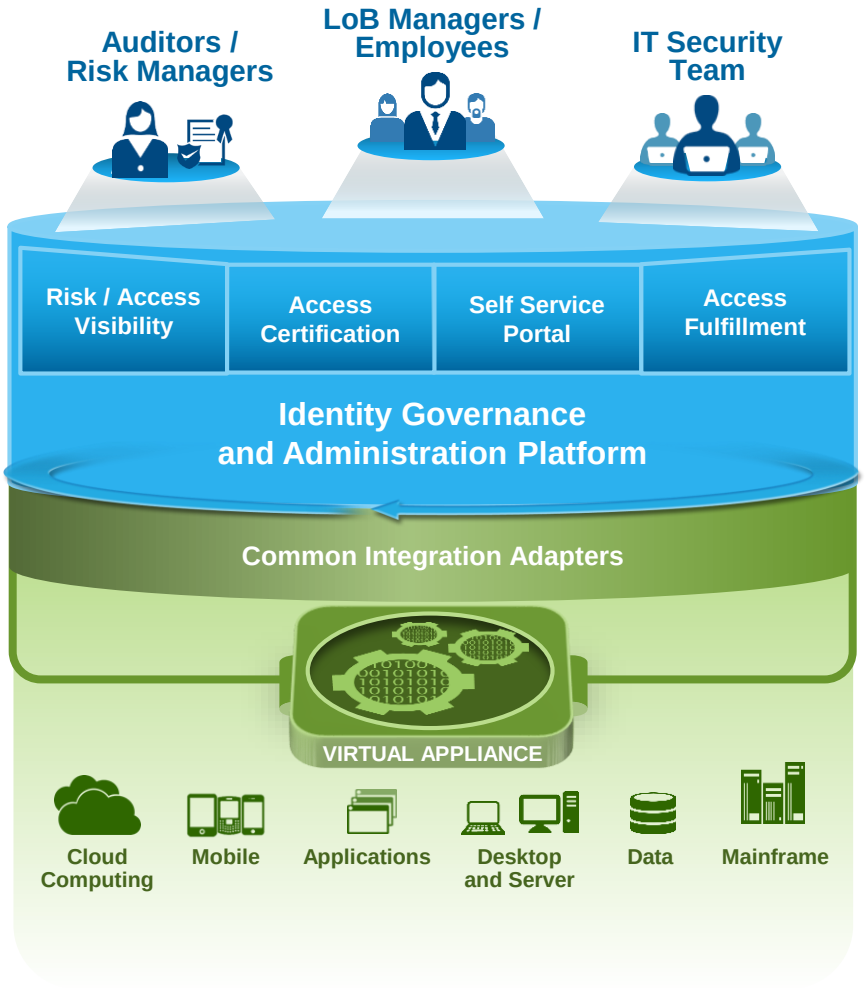
Multinational manufacturer manages over

430M

entitlements

with only a few hundred separation of duty rules

IBM Security Identity Governance and Administration



- **Align Auditors, LoB & IT perspectives** in one consolidated identity governance and administration platform
- **Easy to launch access certification and access request** to meet compliance goals with minimal IT involvement
- **Enhanced role management and separation of duties (SoD) reviews** using visualization dashboard and business-activity mapping
- **In-depth SAP governance** with SoD, access risk and fine-grained entitlements reviews
- **Easy to deploy, virtual appliances for multiple customer adoptions**

Identity and Access Management

Govern and administer users and their access

<Identity Management>
Control unauthorized access and prevent "entitlement creep"

<Access Management>
Validate "who is who" across the enterprise and the cloud

1. ***Is this really a valid user?***
2. ***What does the user want to do?***
3. ***What access does that user need to do their job?***

A new way to think about security

IBM **Security**

Intelligence is the new defense

It helps prevent threats faster and make more informed decisions

Integration is the new foundation

It puts security in context and automates protection

Expertise is the new focus

It is essential to leverage global knowledge and experience to stay ahead

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

Identity and Access Management

Capabilities to help organizations secure the enterprise identity as a new perimeter

Identity Management

- Identity Governance and Intelligence
- User Lifecycle Management
- Privileged Identity Control

Access Management

- Adaptive Access Control and Federation
- Application Content Protection
- Authentication and Single Sign On

Directory Services

IBM Identity and Access Management Solutions and IBM Security Services

Identity and Access Management

Capabilities to help organizations secure the enterprise identity as a new perimeter

Identity Management

- Identity Governance and Intelligence
- User Lifecycle Management
- Privileged Identity Control

Access Management

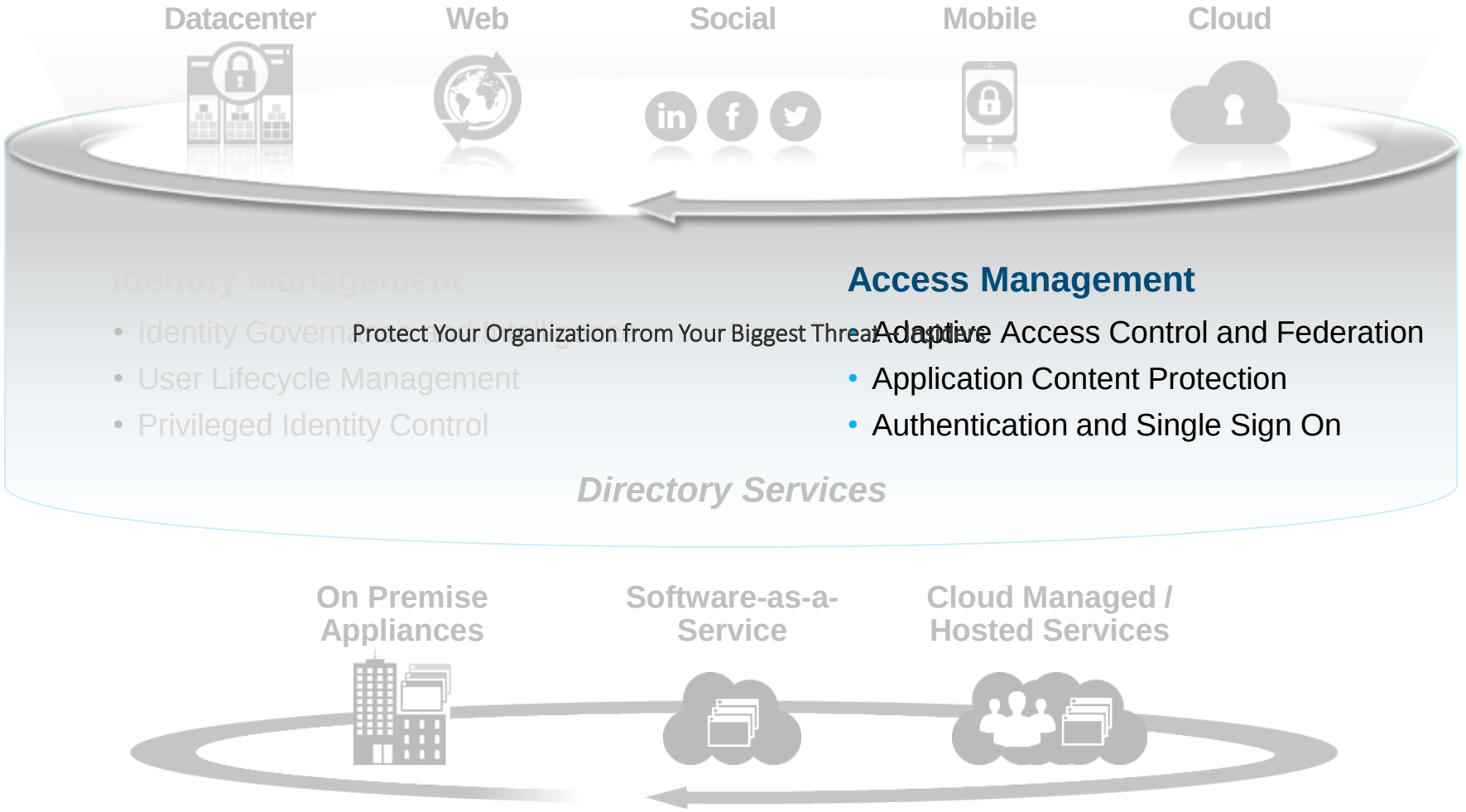
- Adaptive Access Control and Federation
- Application Content Protection
- Authentication and Single Sign On

Directory Services

IBM Identity and Access Management Solutions and IBM Security Services

Identity and Access Management

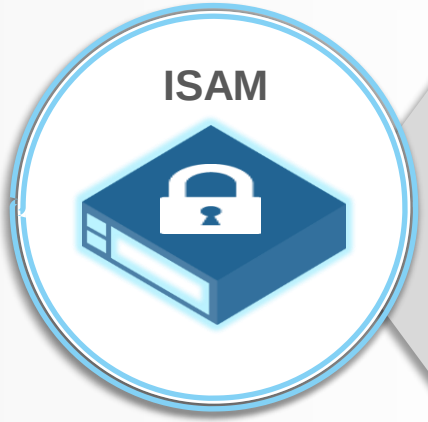
Capabilities to help organizations secure the enterprise identity as a new perimeter



IBM Identity and Access Management Solutions and IBM Security Services

Introducing IBM Security Access Manager 9.0

NEW



New in ISAM 9.0

- Integrated federation capabilities allow single sign-on and access control across on-premise and cloud applications from a single appliance
- Pre-integrated cloud connectors allow for the configuration of cloud application federations in minutes instead of hours or days
- Comprehensive & customizable reporting for ISAM provided by QRadar. Limited use license of QRadar Log Manager is bundled with ISAM 9.0
- Integrated, modular ISAM appliance allows for flexible purchasing, easier deployment and maintenance, and faster time to value

The dependencies of traditional identity management

Business activities vs. Entitlements

Business Manager

Understands what **business activities** employees need

Requests employee IT entitlements from IT Security Manager

Which entitlements grant access to which business activities?

IT Security Manager

Provides information regarding who has which **entitlements**

Who SHOULD have which entitlements?

CRM	ERP
Mainframe	HR
Application Entitlements	

Auditor

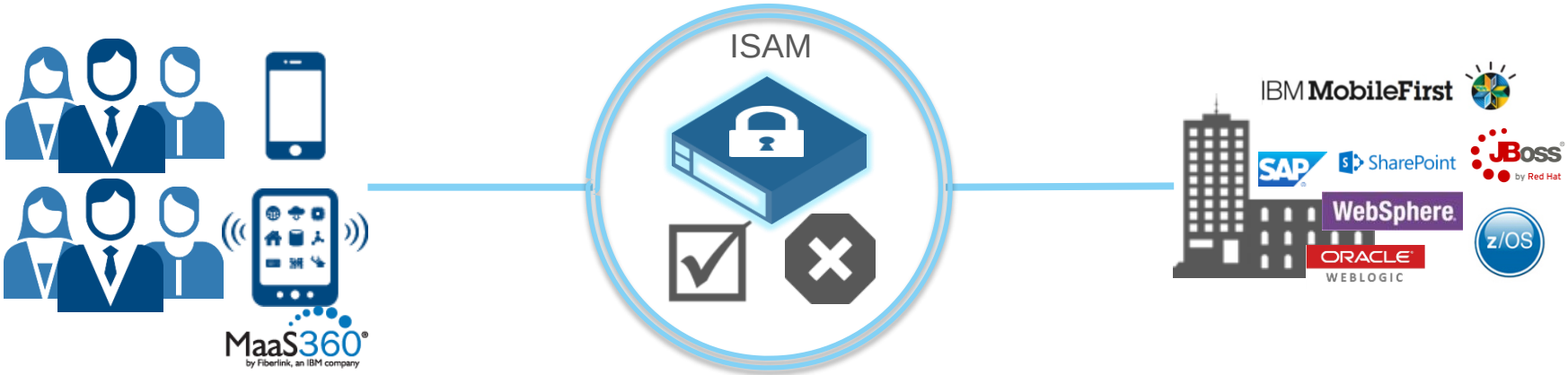
Identifies what **business activities** cause SoD violations *(toxic combinations)*

Receives list of entitlements based on IT Security Manager's request

Which entitlements cause toxic combinations?

2. Seamless user access for enterprise-managed mobile devices

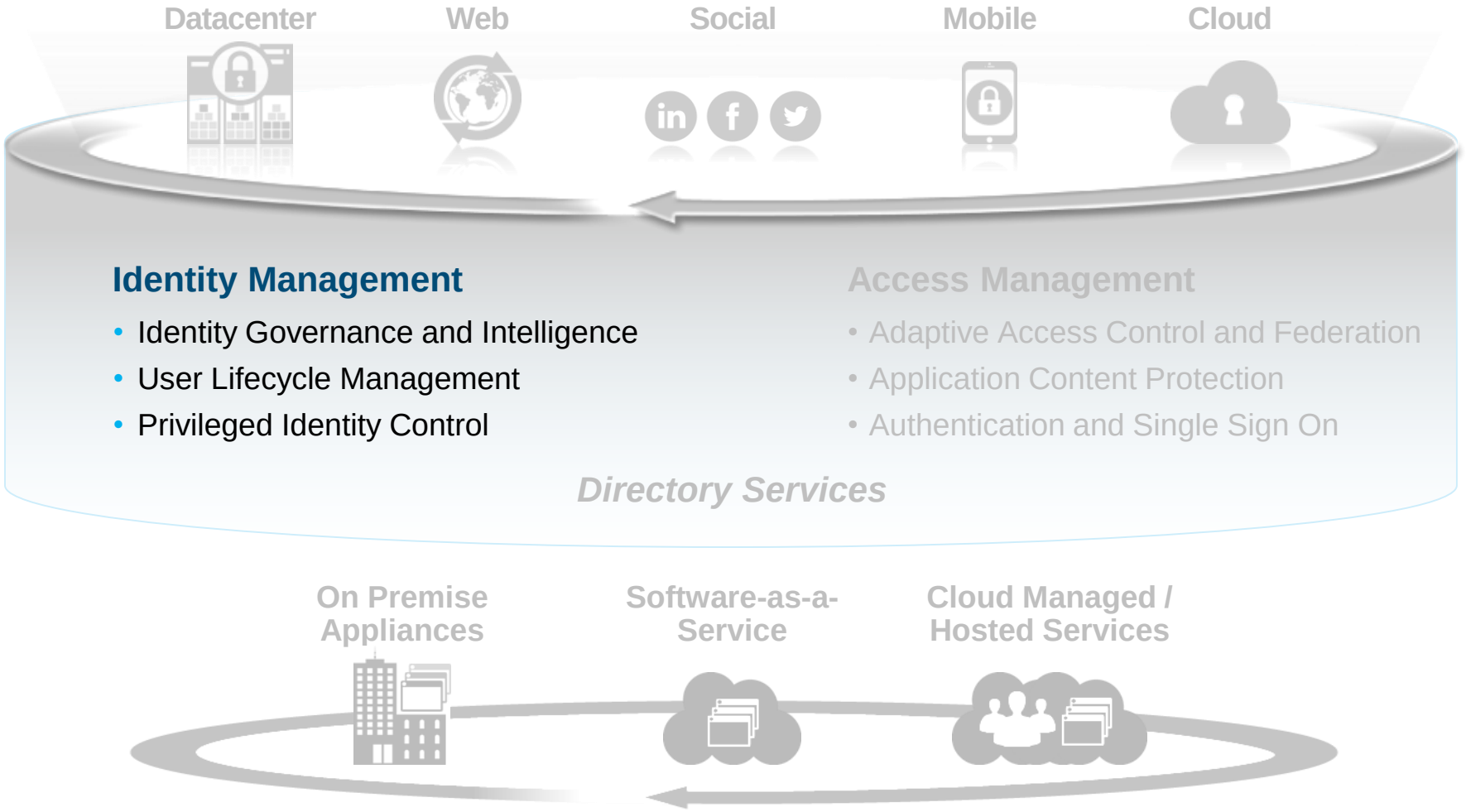
Provide enterprise users with secure mobile access to enterprise applications



- Risk-aware user access secures enterprise infrastructures from unknown and high-risk mobile devices
- Strong and multi-factor authentication capabilities protect critical assets that are accessed by mobile devices off the corporate network

Identity and Access Management

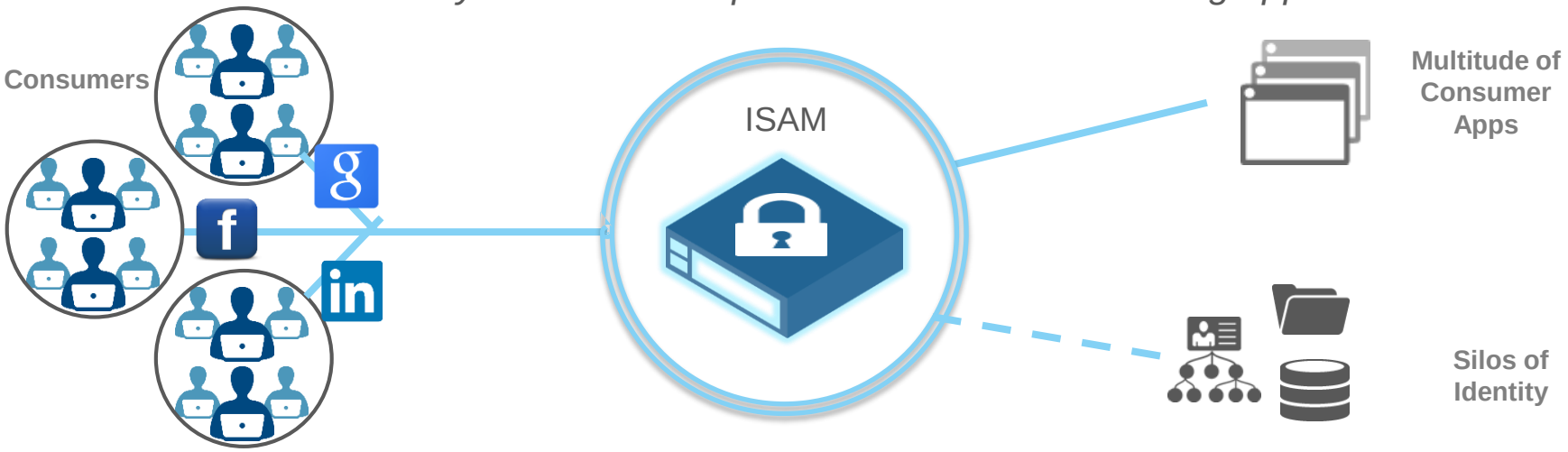
Capabilities to help organizations secure the enterprise identity as a new perimeter



IBM Identity and Access Management Solutions and IBM Security Services

4. Highly scalable consumer identity and access management

Provide user-centric identity and access capabilities for consumer facing applications



- Federate access to multiple consumer-facing applications and deliver an improved end user experience with single sign-on across these properties
- Massively scalable directory and multi-tenant access management platform capable of supporting hundreds of millions of end users
- Self-service focused experience supports end user registration, password and profile management, and social login
- Enhance consumer IAM environment and unify silos of identity with IBM Security Directory Integrator to obtain a single view of the user